The Software Alliance

BSA

全球隐私最佳实践

BSA | 软件联盟是全球领先的软件行业倡导者。如今，软件行业正处于全球尖端创新发展的前沿，其中包括云计算、数据分析和人工智能等。随着基于软件的技术越来越依赖数据，在一些情况下，这些技术需要运用个人数据才能发挥作用。因此，对个人数据进行保护成为了BSA | 软件联盟成员工作的重中之重。我们深知，这是构建客户信任的关键环节。为此，BSA | 软件联盟倡导在保护隐私方面采取一种以用户为中心的应对方法，向个人提供一套能够管理个人数据的机制。此外，BSA还支持制定数据保护框架，确保个人数据的使用与个人预期保持一致，同时让企业能够追求正当的商业利益。

当下，世界各国都在考虑制定数据保护框架，很多国家都在积极探寻解决问题的全球最佳实践。BSA | 软件联盟支持实施增强个人数据收集和使用透明度的最佳实践：通过对个人数据的收集和使用进行管理，尊重和实现知情选择；让个人能够对自己的数据进行管理；提供强大的安全性；推动出于正当商业目的的数据使用。**因此，我们整理了有助于实现以上目标的最佳实践，希望能够推动全球范围内数据保护框架的制定和完善。**

问题	最佳实践
地域范围	数据保护框架应对与一个国家有着足够密切联系的行为进行管理。法律应当适用于以下情形：（1）该国的居民是数据收集与使用的具体目标；（2）作为处理对象的个人数据在收集时是从该国的数据主体中有意收集的；（3）数据的收集是由在该国成立的实体，通过稳定的安排来实施的，由此产生的活动真实有效。
个人数据的定义	个人数据的定义范围应包含与已识别或可识别个人有关的信息。可识别个人是指通过参考标识符，例如姓名、身份证号、位置数据、在线标识符以及个人的身体、心理或基因等身份信息，采取合理手段可以识别的个人。个人数据所覆盖的信息如果处理不当，将会对个人隐私产生重大影响。 通过强大的技术和组织措施进行去识别化处理后，不会涉及重大隐私问题的数据，应从个人数据的定义中排除。
伤害	数据保护框架应根据对个人造成伤害的风险提供定制化的保护。可辨识的伤害应反映身体伤害、对健康的不利影响、财物损失或者是在个人合理预期之外并且很可能造成具体不利后果的敏感个人数据披露。

问题	最佳实践
透明度	数据管理员应就他们对个人数据进行处理的方式方法提供清晰易懂的解释，其中包括所收集的个人数据类别、共享数据的第三方类型，并且应对处理流程进行描述，包含管理员对个人数据的审核、对个人数据进行修改的请求以及获取个人数据副本或删除个人数据的请求等。
目的规范	个人数据应当与以合法方式收集和获取数据的目的相关。管理员应当向个人告知他们收集个人数据的目的，数据的使用方式应当与管理员提供的解释、交易情境或与个人合理预期保持一致，或者与数据收集的最初目的相符。管理员应采用管理系统，确保个人数据的使用和共享符合所述目的。
数据质量	个人数据应与数据的使用目的相关，并且在实现这些目的必要范围内应当是准确的、完整的和最新的。
处理的理由	数据保护框架应能够识别并支持出于一系列正当理由的数据处理，其中包括与交易情境或个人预期保持一致的正当商业目的。其它的正当目的包括：为履行合同而进行的数据处理；出于公众利益或个人切身利益而进行的数据处理；为履行法律义务而进行的数据处理；基于个人同意的数据处理。 数据保护框架不应限制组织机构的以下行为：正当网络安全举措；通过实施相关措施检测、防止欺诈或身份盗窃；保护保密信息；行使合法要求或对合法要求进行抗辩。
同意	管理员应在每次进行个人数据处理时，使个人能够做出知情选择，其行为要与交易情境或组织与个人之间的关系相关。
处理敏感个人数据	特定数据，例如财务账户信息或健康数据，可能特别敏感。如果敏感数据的处理涉及更高的隐私风险，管理员应使被收集敏感数据的个人明确同意。

问题	最佳实践
个人权利	个人应能够请求获取相关信息以了解组织机构是否拥有与他们有关的个人信息以及此类数据的性质。他们应能够对该数据的准确性提出质疑并且酌情要求组织机构对数据进行更正或删除。此外，个人还应能够获得向组织机构提供的或创建的个人数据副本。组织机构应能够迅速确定向个人提供这一信息的适当方式和形式。 确定个人数据处理方式和目的的管理员，应当主要负责对这些请求做出回应。管理员在以下情形中可以拒绝此类请求：比如这样做将产生不合理的负担或费用，或与个人隐私风险不相符；为遵守法律的要求；为确保网络安全；为保护机密的商业信息；出于研究目的；为避免侵犯其他人的隐私、言论自由或其它权利。 管理员还应实施安全验证程序，对提出请求的个人进行验证，从而应对信息披露不当的风险。
安全和泄露通知	管理员和处理者应依据数据的数量和敏感程度、企业的规模和复杂程度以及可用工具的成本，采取合理且适当的安全措施，防止个人数据在未经授权时被访问、销毁、使用、修改或披露。 数据管理员应在发现涉及未经授权获取未加密或未编辑的个人数据泄露时，在切实可行的情况下尽快通知个人，以免造成身份盗窃或财务欺诈的重大风险。作为责任要求的一部分，此类泄露可能需要与组织机构采取的安全措施一起定期报告给监管部门。
责任要求	管理员应制定相关政策和程序，提供此处概述的保障措施，包括：指定人员协调实施相关保障措施的计划，并提供员工培训和管理；定期监测和评估这些方案的执行情况；并在必要时予以调整以解决出现的问题。 作为这些措施的一部分，管理员在处理敏感数据时可以开展定期风险评估，并且在发现重大风险后对相关保护措施的实施进行记录。无需强制要求组织机构向政府部门报告风险评估或事先与政府部门进行协商，因为这会造成不必要的行政管理负担，耽误有价值服务的交付，也不会在隐私保护方面带来益处。

问题	最佳实践
跨境数据传输	数据保护框架应支持和鼓励数据跨境流动，这是全球经济的支柱。在全球范围内传输数据的组织机构应实施相关程序，确保传输到境外的数据继续得到保护。如果数据保护制度之间存在差异，各国政府应创造工具弥补这些差距，既保护隐私，又推动全球数据传输。数据保护框架应禁止公私领域的数据本地化要求，因为这无益于实施安全措施，会阻碍业务创新，限制对个人提供的服务。
管理员和处理者的义务/责任分配	管理员在确定对个人数据进行处理的方式和目的时，应当对满足法律隐私和安全义务负首要责任。代表管理员对数据进行处理的人员应当根据合同约定遵守管理员的指示。管理员和处理者应当能够就他们的合同条款进行灵活的谈判，而非采用法律提供的强制性惯用语言。
补救方法和惩罚措施	集中的监管部门应当拥有所需的工具和资源，确保相关政策有效的强制执行。补救方法和惩罚措施应当与违反数据保护法律造成的伤害相符。民事惩罚不应当任意设定或基于与造成的伤害之间缺乏实质性联系的因素而定。刑事惩罚并非违反数据保护法律的恰当补救方法。